CLAIMS

What is claimed is:

1. A method of selectively enforcing a security policy in a network, the method comprising the computer-implemented steps of:

creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource;

receiving, from an external binding process, a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;

updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and

permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network.

2. A method as recited in Claim 1, wherein the steps of creating and storing one or more access controls in a policy enforcement point that controls access to the network comprise the steps of:

creating and storing one or more definitions of groups in a data store;

creating and storing one or more definitions of resources within a data store;

creating and storing one or more access controls at the policy enforcement point, wherein each of the access controls specifies that a named group is allowed access to a particular resource, and wherein one of the access controls specifies that all other traffic is denied access to the network.

3. A method as recited in Claim 1, further comprising the steps of distributing the network address of the authenticated user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points of a protected network that the user seeks to access.

4. A method as recited in Claim 1, further comprising the steps of distributing the network address of the authenticated user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points that define a security zone that encompasses the user.

5. A method as recited in Claim 1, wherein the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprises the steps of receiving an Internet Protocol (IP) address for the user from a network address binding resolution (NABR) process.

6. A method as recited in Claim 1, further comprising the steps of determining that the user has discontinued use of the client, and deleting the network address to which the user is bound from each named group of each policy enforcement point of the network.

7. A method of selectively enforcing a security policy in a network, the method comprising the computer-implemented steps of:

creating and storing one or more definitions of abstract groups that are authorized to use protected resources of the network, wherein each of the definitions of abstract groups includes an abstract group name and a list of one or more network addresses of authorized users of the protected resources;

creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource;

receiving a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;

determining whether the bound network address of the authenticated user is in one of the lists of one of the named abstract groups; and

permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named abstract group identified in one of the access controls that specifies that the named group is allowed access to the network.

8. A method as recited in Claim 7, wherein the steps of creating and storing one or more access controls in a policy enforcement point that controls access to the network comprise the steps of:
creating and storing one or more definitions of groups in a data store;
creating and storing one or more definitions of resources within a data store;
creating and storing one or more access controls at the policy enforcement point, wherein each of the access controls specifies that a named group is allowed access to a particular resource, and wherein one of the access controls specifies that all other traffic is denied access to the network.

9. A method as recited in Claim 7, further comprising the steps of distributing the network address of the authenticated user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points of a protected network that the user seeks to access.

10. A method as recited in Claim 7, further comprising the steps of distributing the network address of the authenticated user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points that define a security zone that encompasses the user.

11. A method as recited in Claim 7, wherein the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprises the steps of receiving an Internet Protocol (IP) address for the user from a network address binding resolution (NABR) process.

12. A method as recited in Claim 7, further comprising the steps of determining that the user has discontinued use of the client, and deleting the network address to which the user is bound from each named group of each policy enforcement point of the network.

13. A computer-readable medium carrying one or more sequences of instructions for selectively enforcing a security policy in a network, which instructions, when executed by one or more processors, cause the one or more processors to carry out the steps of:

creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource;

receiving a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;

updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and

permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network.

14. A computer-readable medium as recited in Claim 13, wherein the instructions for carrying out the steps of creating and storing one or more access controls in a policy enforcement point that controls access to the network comprise instructions for carrying out the steps of:

creating and storing one or more definitions of groups in a data store;

creating and storing one or more definitions of resources within a data store;

creating and storing one or more access controls at the policy enforcement point, wherein each of the access controls specifies that a named group is allowed access to a particular resource, and wherein one of the access controls specifies that all other traffic is denied access to the network.

15. A computer-readable medium as recited in Claim 13, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of distributing the network address of the authenticated user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points of a protected network that the user seeks to access.

16. A computer-readable medium as recited in Claim 13, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of distributing the network address of the authenticated user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points that define a security zone that encompasses the user.

17. A computer-readable medium as recited in Claim 13, wherein the instructions for carrying out the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprise instructions for carrying out the steps of performing network address binding resolution for the user.

18. A computer-readable medium as recited in Claim 13, further comprising instructions which, when executed by the one or more processors, cause the one or more processors to carry out the steps of determining that the user has discontinued use of the client, and deleting the network address to which the user is bound from each named group of each policy enforcement point of the network.

19. An apparatus for selectively enforcing a security policy in a network, comprising:
means for creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource;

means for receiving a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;

means for updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and

means for permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network.

20. An apparatus for selectively enforcing a security policy in a network, comprising:

a network interface that is coupled to the data network for receiving one or more packet flows therefrom;

a processor;

one or more stored sequences of instructions which, when executed by the processor, cause the processor to carry out the steps of:

creating and storing one or more access controls in a policy enforcement point device that controls access of clients to the network, wherein each of the access controls specifies that a named abstract group is allowed access to a particular resource;

receiving a binding of a network address to an authenticated user of one of the clients for which the policy enforcement point controls access to the network;

updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and

permitting a packet flow originating from the network address to pass from the policy enforcement point into the network only if the network address is in the named group identified in one of the access controls that specifies that the named group is allowed access to the network.

21. A method as recited in Claim 1, wherein the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprises the steps of receiving an Internet Protocol (IP) address for the user from an ASAP protocol process.

22. A method as recited in Claim 1, wherein the steps of receiving a binding of a network address to an authenticated user of a client for which the policy enforcement point controls access to the network comprises the steps of receiving an Internet Protocol (IP) address for the user from a DNS process.

23. A method of selectively enforcing a security policy in a network, the method comprising the computer-implemented steps of:

creating and storing one or more access control list entries in a network router that acts as a policy enforcement point device and that controls a ccess of clients to the network, wherein each of the access control list entries specifies that a named group of users is allowed or refused access to a particular network resource;

creating and storing one or more definitions of the named groups in a data store that is accessible by the network router;

receiving, from an external process that can bind a user to a specific network address, a binding of a network address to an authenticated user of one of the clients for which the router controls access to the network;

updating the named group to include the bound network address of the authenticated user at the policy enforcement point; and

permitting a packet flow originating from the bound network address to pass from the policy enforcement point into the network only if the bound network address is in the named group identified in one of the access control list entries that specifies that the named group is allowed access to the network.

24. A method of selectively enforcing a security policy in a network, the method comprising the computer-implemented steps of:

creating and storing one or more access control list entries in a network router that acts as a policy enforcement point device and that controls access of clients to the network, wherein each of the access control list entries specifies that a named group of users is allowed or refused access to a particular network resource;

creating and storing one or more definitions of the named groups in a data store that is accessible by the network router;

receiving, from an external process that can bind a user to a specific network address, a binding of a network address to an authenticated user of one of the clients for which the router controls access to the network;

updating the named group to include the bound network address of the authenticated user at the policy enforcement point;

permitting a packet flow originating from the bound network address to pass from the policy enforcement point into the network only if the bound network address is in the named group identified in one of the access control list entries that specifies that the named group is allowed access to the network; and

distributing the network address of the authenticated user and information identifying one or more groups of which the authenticated user is a member to all policy enforcement points that define a security zone that encompasses the user;

determining that the user has discontinued use of the client, and deleting the network address to which the user is bound from each named group of each policy enforcement point of the network.